

ETH-Hardness for Symmetric Signaling in Zero-Sum Games

Aviad Rubinstein*

December 2, 2015

Abstract

We prove that, assuming the exponential time hypothesis, finding an ϵ -approximately optimal symmetric signaling scheme in a two-player zero-sum game requires quasi-polynomial time ($n^{\Omega(\lg n)}$). This is tight by [6] and resolves an open question of Dughmi [10]. We also prove that finding a multiplicative approximation is NP-hard.

1 Introduction

Many classical questions in Economics involve extracting information from strategic agents. Recently, there has been growing interest in *signaling*: the study of how to *reveal information* to strategic agents (see e.g. [10, 6] and references therein). Signaling has been studied in many interesting economic and game theoretic settings. Among them, SYMMETRIC ZERO-SUM SIGNALING proposed by Dughmi [10] stands out as a canonical problem that cleanly captures the computational nature of signaling. In particular, focusing on zero-sum games trivializes issues of equilibrium selection and computational tractability of finding an equilibrium.

Definition 1 (SYMMETRIC ZERO-SUM SIGNALING [10]). Alice and Bob play a Bayesian zero-sum game where the payoff matrix is drawn from a publicly known prior. A *signaling scheme* privately observes the state of nature (i.e. the payoff matrix), and then publicly broadcasts a signal to both Alice and Bob. The goal is to design an efficient signaling scheme (a function from payoff matrices to strings) that maximizes Alice’s expected payoff in the induced Nash equilibrium.

Dughmi’s [10] main result proves that assuming the hardness of the Planted Clique problem, there is no additive FPTAS for SYMMETRIC ZERO-SUM SIGNALING. The main open question left by [10] is whether there exists an additive PTAS. Here we answer this question on the negative: we prove that assuming the Exponential Time Hypothesis (ETH) [11], obtaining an additive- ϵ -approximation (for some constant $\epsilon > 0$) requires quasi-polynomial time ($n^{\Omega(\lg n)}$). This result is tight thanks to a recent quasi-polynomial algorithm by Cheng et al. [6]. Another important advantage of our result is that it replaces the hardness of Planted Clique with a more believable worst-case hardness assumption (see e.g. the discussion in [5]).

Using a similar construction, we also obtain NP-hardness for computing a multiplicative- $(1 - \epsilon)$ -approximation. Unfortunately our game uses both negative and positive payoffs, which

*UC Berkeley. I thank Shaddin Dughmi for explaining [6], and Christos Papadimitriou for comments on an earlier draft. This research was supported by Microsoft Research PhD Fellowship, as well as NSF grant CCF1408635 and by Templeton Foundation grant 3966. This work was done in part at the Simons Institute for the Theory of Computing.

is somewhat non-standard (but not unprecedented [7]) in multiplicative approximation. However, we note that the purpose of negative and positive payoffs is only to obtain structural constraints on the resulting equilibria; the hardness of approximation is not a result of cancellation of negative with positive payoffs: Alice’s payoff can be decomposed as a difference of non-negative payoffs $U = U^+ - U^-$, such that it is hard to approximate Alice’s optimal payoff to within $\epsilon \cdot \mathbb{E}[U^+ + U^-]$. Nevertheless, we believe that extending this result to non-negative payoffs could be very interesting.

Finally, we note that since all our games are zero-sum, our hardness results carry over to the respective notions of additive- and multiplicative- ϵ -Nash equilibrium.

1.1 Techniques

Our main ingredient for the quasi-polynomial hardness is the technique of “birthday repetition” coined by [1] and recently applied in game theoretic settings in [5, 3]: We reduce from a constraint satisfaction problem (CSP) over n variables to a distribution over N zero-sum $N \times N$ games, with $N = 2^{\Theta(\sqrt{n})}$. Alice and Bob’s strategies correspond to assignments to tuples of \sqrt{n} variables. By the birthday paradox, the two \sqrt{n} -tuples chosen by Alice and Bob share a constraint with constant probability. If a constant fraction of the constraints are unsatisfiable, Alice’s payoff will suffer with constant probability. Assuming ETH, approximating the value of the CSP requires time $2^{\tilde{\Omega}(n)} = N^{\tilde{\Omega}(\lg N)}$.

The challenge The main difficulty is that once the signal is public, the zero-sum game is tractable. Thus we would like to force the signaling scheme to output a satisfying assignment. Furthermore, if the scheme would output partial assignments on different states of nature, it is not clear how to check consistency between different signals. Thus we would like each signal to contain an entire satisfying assignment. The optimal scheme may be very complicated and even require randomization, yet by an application of the Caratheodory Theorem the number of signals is, wlog, bounded by the number of states of nature [10]. If the state of nature can be described using only $\lg N = \tilde{\Theta}(\sqrt{n})$ bits, how can we force the scheme to output an entire assignment?

To overcome this obstacle, we let the state of nature contain a partial assignment to a random \sqrt{n} -tuple of variables. We then check the consistency of Alice’s assignment with nature’s assignment, Bob’s assignment with nature’s assignment, and Alice and Bob’s assignments with each other; let $\tau^{A,Z}, \tau^{B,Z}, \tau^{A,B}$ denote the outcomes of those consistency checks, respectively. Alice’s payoff is given by:

$$U = \delta \tau^{A,Z} - \delta^2 \tau^{B,Z} + \delta^3 \tau^{A,B}$$

for some small constant $0 < \delta < 1$. Now, both Alice and Bob want to maximize their chances of being consistent with nature’s partial assignment, and the signaling scheme gains by maximizing $\tau^{A,B}$.

Of course, if nature outputs a random assignment, we have no reason to expect that it can be completed to a full satisfying assignment. Instead, the state of nature consists of N assignments, and the signaling scheme helps Alice and Bob play with the assignment that can be completed.

Several other obstacles arise; fortunately some can be handled using techniques from previous works on hardness of finding Nash equilibrium [2, 8, 3].

2 Preliminaries

PCP Theorem

Theorem 1 (PCP Theorem [9]; see e.g. [4, Theorem 2.11] for this formulation). *Given a 3SAT instance φ of size n , there is a polynomial time reduction that produces a 2CSP instance ψ , with size $|\psi| = n \cdot \text{polylog} n$ variables and constraints, and constant alphabet size, such that:*

Completeness *If φ is satisfiable, then so is ψ .*

Soundness *If φ is not satisfiable, then at most a $(1 - \eta)$ -fraction of the constraints in ψ can be satisfied, for some $\eta = \Omega(1)$.*

Balance *Every variable in ψ participates in exactly $d = O(1)$ constraints.*

Finding a good partition

Lemma 1 (Essentially [3, Lemma 6]). *Given a d -regular graph $G = (V, E)$, we can partition V into $|V|/k$ disjoint subsets $\{S_1, \dots, S_{|V|/k}\}$ of size at most $2k$ such that:*

$$\forall i, j \quad |(S_i \times S_j) \cap E| \leq 8d^2k^2/n \quad (1)$$

Proof. We assign vertices to subsets iteratively, and show by induction that we can always maintain (1) and the bound on the subset size. Since the average set size is less than k , we have by Markov's inequality that at each step less than half of the subsets are full. The next vertex we want to assign, v , has neighbors in at most d subsets. By our induction hypothesis, each S_i is of size at most $2k$, so in expectation over $j \in [n]$, it has less than $4dk^2/n$ neighbors in each S_j . Applying Markov's inequality again, S_i has at least $8d^2k^2/n$ neighbors in less than a $(1/2d)$ -fraction of subsets S_j . In total, we ruled out less than half of the subsets for being full, and less than half of the subsets for having too many neighbors with subsets that contain neighbors of v . Therefore there always exists some subset S_i to which we can add v while maintaining the induction hypothesis. \square

How to catch a far-from-uniform distribution

Lemma 2 (Lemma 3 in the full version of [8]). *Let $\{a_i\}_{i=1}^n$ be real numbers satisfying the following properties for some $\theta > 0$: (1) $a_1 \geq a_2 \geq \dots \geq a_n$; (2) $\sum a_i = 0$; (3) $\sum_{i=1}^{n/2} a_i \leq \theta$. Then $\sum_{i=1}^n |a_i| \leq 4\theta$.*

3 Additive hardness

Theorem 2. *There exists a constant $\epsilon > 0$, such that assuming ETH, approximating SYMMETRIC ZERO-SUM SIGNALING with payoffs in $[-1, 1]$ to within an additive ϵ requires time $n^{\tilde{\Omega}(\lg n)}$.*

Construction overview

Our reduction begins with a 2CSP ψ over n variables from alphabet Σ . We partition the variables into n/k disjoint subsets $\{S_1, \dots, S_{n/k}\}$, each of size at most $2k$ for $k = \sqrt{n}$ such that every two subsets share at most a constant number of constraints.

Nature chooses a random subset S_i from the partition, a random assignment $\vec{u} \in \Sigma^{2k}$ to the variables in S_i , and an auxiliary vector $\hat{b} \in \{0, 1\}^{\Sigma \times [2k]}$. As mentioned in Section 1.1, \vec{u} may not correspond to any satisfying assignment. Alice and Bob participate in one of $|\Sigma|^{2k}$ subgames; for each $\vec{v} \in \Sigma^{2k}$, there is a corresponding subgame where all the assignments are XOR-ed with \vec{v} . The optimum signaling scheme reveals partial information about \hat{b} in a way that guides Alice and Bob to participate in the subgame where the XOR of \vec{v} and \vec{u} can be completed to a full satisfying assignment. The scheme also outputs the full satisfying assignment, but reveals no information about the subset S_i chosen by nature.

Each player has $\left(|\Sigma|^{2k} \times 2\right) \times \left(n/k \times \binom{n/k}{n/2k} \times |\Sigma|^{2k}\right) = 2^{\Theta(\sqrt{n})}$ strategies. The first $|\Sigma|^{2k}$ strategies correspond to a Σ -ary vector \vec{v} that the scheme will choose after observing the random input. The signaling scheme forces both players to play (w.h.p.) the strategy corresponding to \vec{v} by controlling the information that corresponds to the next 2 strategies. Namely, for each $\vec{v}' \in \Sigma^{2k}$, there is a random bit $b(\vec{v}')$ such that each player receives a payoff of 1 if they play $(\vec{v}', b(\vec{v}'))$ and 0 for $(\vec{v}', 1 - b(\vec{v}'))$. The b 's are part of the state of nature, and the signaling scheme will reveal only the bit corresponding to the special \vec{v} . Since there are $|\Sigma|^{2k}$ bits, nature cannot choose them independently, as that would require $2^{|\Sigma|^{2k}}$ states of nature. Instead we construct a pairwise independent distribution.

The next n/k strategies correspond to the choice of a subset S_i from the specified partition of variables. The $\binom{n/k}{n/2k}$ strategies that follow correspond to a gadget due to Althofer [2] whereby each player forces the other player to randomize (approximately) uniformly over the choice of subset.

The last $|\Sigma|^{2k}$ strategies correspond to an assignment to S_i . The assignment to each S_i is XOR-ed entry-wise with \vec{v} . Then, the players are paid according to checks of consistency between their assignments, and a random assignment to a random S_i picked by nature. (The scheme chooses \vec{v} so that nature's random assignment is part of a globally satisfying assignment.) Each player wants to pick an assignment that passes the consistency check with nature's assignment. Alice also receives a small bonus if her assignment agrees with Bob's; thus her payoff is maximized when there exists a globally satisfying assignment.

Formal construction

Let ψ be a 2CSP- d over n variables from alphabet Σ , as guaranteed by Theorem 1. In particular, ETH implies that distinguishing between a completely satisfiable instance and $(1 - \eta)$ -satisfiable requires time $2^{\tilde{\Omega}(n)}$. By Lemma 1, we can (deterministically and efficiently) partition the variables into n/k subsets $\{S_1, \dots, S_{n/k}\}$ of size at most $2k = 2\sqrt{n}$, such that every two subsets share at most $8d^2k^2/n = O(1)$ constraints.

States of nature Nature chooses a state $(\hat{b}, i, \vec{u}) \in \{0, 1\}^{\Sigma \times [2k]} \times [n/k] \times \Sigma^{2k}$ uniformly at random. For each \vec{v} , $b(\vec{v})$ is the XOR of bits from \hat{b} that correspond to entries of \vec{v} :

$$\forall \vec{v} \in \Sigma^{2k} \quad b(\vec{v}) \triangleq \left(\bigoplus_{(\sigma, \ell): [\vec{v}]_\ell = \sigma} [\hat{b}]_{(\sigma, \ell)} \right).$$

Notice that the $b(\vec{v})$'s are pairwise independent and each marginal distribution is uniform over $\{0, 1\}$.

Strategies Alice and Bob each choose a strategy $(\vec{v}, c, j, T, \vec{w}) \in \Sigma^{2k} \times \{0, 1\} \times [n/k] \times \binom{[n/k]}{n/2k} \times \Sigma^{2k}$. We use \vec{v}^A, c^A , etc. to denote the strategy Alice plays, and similarly \vec{v}^B, c^B , etc. for Bob. For $\sigma, \sigma' \in \Sigma$, we denote $\sigma \oplus_\Sigma \sigma' \triangleq \sigma + \sigma' \pmod{|\Sigma|}$, and for vectors $\vec{v}, \vec{v}' \in \Sigma^{2k}$, we let $\vec{v} \oplus_\Sigma \vec{v}' \in \Sigma^{2k}$ denote the entry-wise \oplus_Σ . When $\vec{v}^A = \vec{v}^B = \vec{v}$, we set $\tau^{A,Z} = 1$ if assignments $(\vec{v} \oplus_\Sigma \vec{w}^A)$ and $(\vec{v} \oplus_\Sigma \vec{u})$ to subsets S_i and S_{j^A} , respectively, satisfy all the constraints in ψ that are determined by $(S_i \cup S_{j^A})$, and $\tau^{A,Z} = 0$ otherwise. Similarly, $\tau^{B,Z} = 1$ iff $(\vec{v} \oplus_\Sigma \vec{w}^B)$ and $(\vec{v} \oplus_\Sigma \vec{u})$ satisfy the corresponding constraints in ψ ; and $\tau^{A,B}$ checks $(\vec{v} \oplus_\Sigma \vec{w}^A)$ and $(\vec{v} \oplus_\Sigma \vec{w}^B)$. When $\vec{v}^A \neq \vec{v}^B$, we set $\tau^{A,Z} = \tau^{B,Z} = \tau^{A,B} = 0$.

Payoffs Given state of nature (\hat{b}, i, \vec{u}) and players' strategies $(\vec{v}^A, c^A, j^A, T^A, \vec{w}^A)$ and $(\vec{v}^B, c^B, j^B, T^B, \vec{w}^B)$, We decompose Alice's payoff as:

$$U^A \triangleq U_b^A + U_{\text{Althofer}}^A + U_\psi^A,$$

where

$$U_b^A \triangleq \mathbf{1}\{c^A = b(\vec{v}^A)\} - \mathbf{1}\{c^B = b(\vec{v}^B)\},$$

$$U_{\text{Althofer}}^A \triangleq \mathbf{1}\{j^B \in T^A\} - \mathbf{1}\{j^A \in T^B\},$$

and

$$U_\psi^A \triangleq \delta \tau^{A,Z} - \delta^2 \tau^{B,Z} + \delta^3 \tau^{A,B},$$

for a sufficiently small constant $0 < \delta \ll \sqrt{\eta}$.

Completeness

Lemma 3. *If ψ is satisfiable, there exists a signaling scheme and a mixed strategy for Alice that guarantees expected payoff $\delta - \delta^2 + \delta^3$.*

Proof. Fix a satisfying assignment $\vec{\alpha} \in \Sigma^n$. Given state of nature (\hat{b}, i, \vec{u}) , let \vec{v} be such that $(\vec{v} \oplus_\Sigma \vec{u}) = [\vec{\alpha}]_{S_i}$. For each $j \in [n/k]$, let $\vec{\beta}_j$ be such that $(\vec{v} \oplus_\Sigma \vec{\beta}_j) = [\vec{\alpha}]_{S_j}$. (Notice that $\vec{\beta}_i = \vec{u}$.) The scheme outputs the signal $(\vec{v}, b(\vec{v}), \vec{\beta}_1, \dots, \vec{\beta}_{n/k})$. Alice's mixed strategy sets $(\vec{v}^A, c^A) = (\vec{v}, b(\vec{v}))$; picks j^A and T^A uniformly at random; and sets $\vec{w}^A = \vec{\beta}_{j^A}$.

Because Bob has no information about $b(\vec{v}')$ for any $\vec{v}' \neq \vec{v}$, he has probability $1/2$ of losing whenever he picks $\vec{v}^B \neq \vec{v}$, i.e. $\mathbb{E}[U_b^A] \geq \frac{1}{2} \Pr[\vec{v}^B \neq \vec{v}]$. Furthermore, because Alice chooses T^A and j^A uniformly, $\mathbb{E}[U_{\text{Althofer}}^A] = 0$.

Since $\vec{\alpha}$ completely satisfies ψ , we have that $\tau^{A,Z} = 1$ as long as $\vec{v}^B = \vec{v}$ (regardless of the rest of Bob's strategy). Bob's goal is thus to maximize $\delta^2 \tau^{B,Z} - \delta^3 \tau^{A,B}$. However, since Alice's assignment and nature's assignment are drawn from the same distribution, we have that for any mixed strategy that Bob plays, $\mathbb{E}[\tau^{B,Z}] = \mathbb{E}[\tau^{A,B}]$. Therefore Alice's payoff is at least

$$(\delta - \delta^2 + \delta^3) \Pr[\vec{v}^B = \vec{v}] + \frac{1}{2} \Pr[\vec{v}^B \neq \vec{v}] \geq \delta - \delta^2 + \delta^3.$$

□

Soundness

Lemma 4. *If at most a $(1 - \eta)$ -fraction of the constraints are satisfiable, Alice's maxmin payoff is at most $\delta - \delta^2 + (1 - \Omega(1))\delta^3$, for any signaling scheme.*

Proof. On any signal, Bob chooses (\vec{v}^B, c^B) from the same distribution that Alice uses for (\vec{v}^A, c^A) . He chooses j^B uniformly, and picks T^B so as to minimize $\mathbb{E}[U_{\text{Althofer}}^A]$. Finally, for each j^B , he draws \vec{w}^B from the same marginal distribution that Alice uses for \vec{w}^A conditioning on $j^A = j^B$ (and uniformly at random if Alice never plays $j^A = j^B$). By symmetry, $\mathbb{E}[U_b^A] = 0$ and $\mathbb{E}[U_{\text{Althofer}}^A] \leq 0$.

In Althofer's gadget, Alice can guarantee an (optimal) expected payoff of 0 by randomizing uniformly over her choice of j^A and T^A . On the converse, by Lemma 2, if Alice's marginal distribution over the choice of j^A is $8\delta^2$ -far from uniform (in total variation distance), then $\mathbb{E}[U_{\text{Althofer}}^A] \leq -2\delta^2$; but this would imply $\mathbb{E}[U^A] \leq -2\delta^2 + \mathbb{E}[U_\psi^A] \leq \delta - 2\delta^2 + \delta^3$, regardless of U_ψ^A . So henceforth we assume wlog that Alice's marginal distribution over the choice of j^A is $O(\delta^2)$ -close to uniform.

Since Alice's marginal distribution over j^A is $O(\delta^2)$ -close to uniform, we have that Bob's distribution over (j^B, \vec{w}^B) is $O(\delta^2)$ -close to Alice's distribution over (j^A, \vec{w}^A) . Therefore $\tau^{B,Z} \geq \tau^{A,Z} - O(\delta^2)$, and so we also get:

$$\mathbb{E}[U^A] \leq \mathbb{E}[U_\psi^A] \leq \delta - \delta^2 + \delta^3 \tau^{A,B} + O(\delta^4). \quad (2)$$

It remains to upper bound $\tau^{A,B}$. By the premise, any assignment to all variables violates at least an η -fraction of the constraints. In particular, this is true in expectation for assignments drawn according to Bob's mixed strategy. Since every pair of subsets shares at most a constant number of constraints, an $\Omega(\eta)$ -fraction of the pairs of assignments chosen by Alice and Bob would violate ψ . Therefore, since Alice's distribution over j^A is $O(\delta^2)$ -close to uniform, we have $\tau^{A,B} \leq 1 - \Omega(\eta) + O(\delta^2)$. Plugging into (2) completes the proof. \square

4 Multiplicative hardness

Theorem 3. *There exists a constant $\epsilon > 0$, such that it is NP-hard to approximate SYMMETRIC ZERO-SUM SIGNALING to within a multiplicative $(1 - \epsilon)$ factor.*

Construction overview

Our reduction begins with a 2CSP ψ over n variables from alphabet Σ .

Nature chooses a random index $i \in [n]$, a random assignment $u \in \Sigma$ for variable x_i , and an auxiliary vector $\vec{b} \in \{0, 1\}^\Sigma$. Notice that u may not correspond to any satisfying assignment. Alice and Bob participate in one of $|\Sigma|$ subgames; for each $v \in \Sigma$, there is a corresponding subgame where all the assignments are XOR-ed with v . The optimum signaling scheme reveals partial information about \vec{b} in a way that guides Alice and Bob to participate in the subgame where the XOR of v and u can be completed to a full satisfying assignment. The scheme also outputs the full satisfying assignment, but reveals no information about the index i chosen by nature.

Alice has $(|\Sigma| \times 2) \times (n \times n \times |\Sigma|) = \Theta(n^2)$ strategies, and Bob has an additional choice among n strategies (so $\Theta(n^3)$ in total). The first $|\Sigma|$ strategies correspond to a value $v \in \Sigma$ that the scheme will choose after observing the state of nature. The signaling scheme forces

both players to play (w.h.p.) the strategy corresponding to v by controlling the information that corresponds to the next 2 strategies. Namely, for each $v' \in \Sigma$, there is a random bit $b(v')$ such that each player receives a small bonus if they play $(v', b(v'))$ and not $(v', 1 - b(v'))$. The b 's are part of the state of nature, and the signaling scheme will reveal only the bit corresponding to the special v .

The next n strategies correspond to a choice of a variable $j \in [n]$. The n strategies that follow correspond to a hide-and-seek gadget whereby each player forces the other player to randomize (approximately) uniformly over the choice of j . For Bob, the additional n strategies induce a hide-and-seek game against nature, which serves to verify that the scheme does not reveal too much information about the state of nature (this extra verification was unnecessary in the reduction for additive inapproximability).

The last $|\Sigma|$ strategies induce an assignment for x_j . The assignment to each x_j is XOR-ed with v . Then, the players are paid according to checks of consistency between their assignments, and a random assignment to a random x_i picked by nature. (The scheme chooses v so that nature's random assignment is part of a globally satisfying assignment.) Each player wants to pick an assignment that passes the consistency check with nature's assignment. Alice also receives a small bonus if her assignment agrees with Bob's; thus her payoff is maximized when there exists a globally satisfying assignment.

Formal construction

Let ψ be a 2CSP- d over n variables from alphabet Σ , as guaranteed by Theorem 1. In particular, it is NP-hard to distinguish between ψ which is completely satisfiable, and one where at most a $(1 - \eta)$ -fraction of the constraints can be satisfied. We denote $(i, j) \in \psi$ if there is a constraint over variables (x_i, x_j) .

States of nature Nature chooses a state $(\vec{b}, i, u) \in \{0, 1\}^\Sigma \times [n] \times \Sigma$ uniformly at random.

Strategies Alice chooses a strategy $(v^A, c^A, j^A, t^A, w^A) \in \Sigma \times \{0, 1\} \times [n] \times [n] \times \Sigma$, and Bob chooses $(v^B, c^B, j^B, t^B, q^B, w^B) \in \Sigma \times \{0, 1\} \times [n] \times [n] \times [n] \times \Sigma$. For $\sigma, \sigma' \in \Sigma$, we denote $\sigma \oplus_\Sigma \sigma' \triangleq \sigma + \sigma' \pmod{|\Sigma|}$, and for a vector $\vec{\alpha} \in \Sigma^n$ we let $(\sigma \oplus_\Sigma \vec{\alpha}) \in \Sigma^n$ denote the \oplus_Σ of σ with each entry of $\vec{\alpha}$. When $v^A = v^B = v$, we set $\tau^{A,Z} = 1$ if ψ contains a constraint for variables (j^A, i) , and the assignments $(v \oplus_\Sigma w^A)$ and $(v \oplus_\Sigma u)$ to those variables, respectively, satisfy this constraint, and $\tau^{A,Z} = 0$ otherwise. Similarly, $\tau^{B,Z} = 1$ iff $(v \oplus_\Sigma w^B)$ and $(v \oplus_\Sigma u)$ satisfy a corresponding constraint in ψ ; and $\tau^{A,B}$ checks $(v \oplus_\Sigma w^A)$ with $(v \oplus_\Sigma w^B)$. When $v^A \neq v^B$, we set $\tau^{A,Z} = \tau^{B,Z} = \tau^{A,B} = 0$.

Payoffs Given players' strategies $(v^A, c^A, j^A, t^A, w^A)$ and $(v^B, c^B, j^B, t^B, q^B, w^B)$ and state of nature (\vec{b}, i, u) , We decompose Alice's payoff as:

$$U^A \triangleq U_b^A + U_{\text{seek}}^A + U_\psi^A,$$

where

$$\begin{aligned} U_b^A &\triangleq \mathbf{1}\{c^A = b(\vec{v}^A)\} / n - \mathbf{1}\{c^B = b(\vec{v}^B)\} / n, \\ U_{\text{seek}}^A &\triangleq 2 \cdot \mathbf{1}\{j^B = t^A\} - \mathbf{1}\{j^A = t^B\} - \mathbf{1}\{i = q^B\}, \end{aligned}$$

and

$$U_\psi^A \triangleq \delta^3 \tau^{A,Z} - \delta^4 \tau^{B,Z} + \delta^5 \tau^{A,B},$$

for a sufficiently small constant $0 < \delta \ll \sqrt{\eta}$.

Completeness

Lemma 5. *If ψ is satisfiable, there exists a signaling scheme and a mixed strategy for Alice that guarantees expected payoff $\frac{d}{n} (\delta^3 - \delta^4 + \delta^5)$.*

Proof. Fix a satisfying assignment $\vec{\alpha} \in \Sigma^n$. Given state of nature (\hat{b}, i, u) , let v be such that $(v \oplus_\Sigma u) = [\vec{\alpha}]_i$, and let $\vec{\beta}$ be such that $(v \oplus_\Sigma \vec{\beta}) = \vec{\alpha}$. (Notice that $[\vec{\beta}]_i = u$.) The scheme outputs the signal $(v, \vec{b}_v, \vec{\beta})$. Alice's mixed strategy sets $(v^A, c^A) = (v, \vec{b}_v)$; picks j^A and t^A uniformly at random; and sets $w^A = [\vec{\beta}]_{j^A}$.

Because Bob has no information about $[\vec{b}]_{v'}$ for any $v' \neq v$, he has probability $1/2$ of losing whenever he picks $v^B \neq v$, i.e. $\mathbb{E}[U_b^A] \geq \frac{1}{2n} \Pr[v^B \neq v]$. Furthermore, because Alice and nature draw t^A, j^A and i uniformly at random, $\mathbb{E}[U_{\text{seek}}^A] = 0$.

Since $\vec{\alpha}$ completely satisfies ψ , we have that $\mathbb{E}[\tau^{A,Z}] = \Pr[(j^A, i) \in \psi] = d/n$, as long as $v^B = v$ (regardless of the rest of Bob's strategy). Bob's goal is thus to maximize $\delta^4 \tau^{B,Z} - \delta^5 \tau^{A,B}$. However, since Alice's assignment and nature's assignment are drawn from the same distribution, we have that for any mixed strategy Bob plays, $\mathbb{E}[\tau^{B,Z}] = \mathbb{E}[\tau^{A,B}]$. Finally, since i is a uniformly random index, $\mathbb{E}[\tau^{B,Z}] \leq d/n$. Therefore Alice's payoff is at least

$$\frac{d}{n} (\delta^3 - \delta^4 + \delta^5) \Pr[v^B = v] + \frac{1}{2n} \Pr[v^B \neq v] \geq \frac{d}{n} (\delta^3 - \delta^4 + \delta^5).$$

□

Soundness

Lemma 6. *When at most a $(1 - \eta)$ -fraction of the constraints are satisfiable, for any signaling scheme, Alice's maxmin payoff is at most $\frac{d}{n} (\delta^3 - \delta^4 + (1 - \Omega(1)) \delta^5)$.*

Proof. On any signal, Bob chooses (v^B, c^B) from the same distribution that Alice uses for (v^A, c^A) . He draws j^B uniformly at random, and picks t^B and q^B so as to minimize $\mathbb{E}[U_{\text{seek}}^A]$. Finally, for each j^B , Bob draws w^B from the same distribution that Alice uses for w^A conditioning on $j^A = j^B$ (and uniformly at random if Alice never plays $j^A = j^B$). By symmetry, $\mathbb{E}[U_b^A] = 0$ and $\mathbb{E}[U_{\text{seek}}^A] \leq 0$.

Notice that

$$\mathbb{E}[U_\psi^A] \leq \delta^3 \cdot \Pr[(i, j^A) \in \psi] + \delta^5 \cdot \frac{d}{n}. \quad (3)$$

We can assume wlog that $\Pr[(i, j^A) \in \psi] \leq 3d/n$. Otherwise, Bob can draw \hat{j}^A from the same marginal distribution that Alice uses for j^A , and set q^B to a random ψ -neighbor of \hat{j}^A . This would imply $\Pr[i = q^B] \geq \Pr[(i, j^A) \in \psi] / d$, and therefore

$$\begin{aligned} \mathbb{E}[U_{\text{seek}}^A] &\leq 2/n - \Pr[(i, j^A) \in \psi] / d \\ &\leq -\Pr[(i, j^A) \in \psi] / 3d \\ &\leq -\mathbb{E}[U_\psi^A], \end{aligned}$$

in which case $\mathbb{E}[U^A] \leq 0$. Therefore by (3), $\mathbb{E}[U_\psi^A] \leq 4d\delta^3/n$.

Furthermore, we claim that Alice's optimal marginal distribution over the choice of j^A is $O(\delta^3)$ -close to uniform (in total variation distance). Suppose by contradiction that the distribution is $8d\delta^3$ -far from uniform. Then there exists some $\ell \in [n]$ such that $\Pr[j^A = \ell] \geq (1 + 4d\delta^3)/n$. If Bob always plays $t^B = \ell$, then $\mathbb{E}[U_{\text{seek}}^A] \leq -4d\delta^3/n$, and $\mathbb{E}[U^A] \leq 0$.

Since Alice's distribution over j^A is $O(\delta^3)$ -close to uniform, we have that Bob's distribution over (j^B, w^B) is $O(\delta^3)$ -close to Alice's distribution over (j^A, w^A) . Therefore, $\tau^{B,Z} \geq \tau^{A,Z} - O(\delta^3)$, so

$$\begin{aligned} \delta^3 \tau^{A,Z} - \delta^4 \tau^{B,Z} &\leq (\delta^3 - \delta^4 + O(\delta^7)) \cdot \Pr[(i, j^A) \in \psi] \\ &\leq \frac{d}{n} (\delta^3 - \delta^4 + O(\delta^6)) \end{aligned}$$

We now upper bound $\tau^{A,B}$. By the premise, any assignment to all variables violates at least an η -fraction of the constraints. In particular, this is true in expectation for assignments drawn according to Bob's mixed strategy. Therefore, since Alice's marginal distribution over j^A is $O(\delta^3)$ -close to uniform, we have that

$$\tau^{A,B} \leq (1 - \Omega(\eta) + O(\delta^3)) \cdot \Pr[(j^A, j^B) \in \psi] \leq \frac{d}{n} (1 - \Omega(\eta) + O(\delta^3)).$$

Thus in total

$$\mathbb{E}[U^A] \leq \mathbb{E}[U_\psi^A] \leq \frac{d}{n} (\delta^3 - \delta^4 + (1 - \Omega(\eta))\delta^5 + O(\delta^6)).$$

□

References

- [1] Scott Aaronson, Russell Impagliazzo, and Dana Moshkovitz. AM with multiple merlins. In *Computational Complexity (CCC), 2014 IEEE 29th Conference on*, pages 44–55. IEEE, 2014.
- [2] Ingo Althofer. On sparse approximations to randomized strategies and convex combinations. 1993.
- [3] Yakov Babichenko, Christos H. Papadimitriou, and Aviad Rubinstein. Can almost everybody be almost happy? PCP for PPAD and the inapproximability of nash. *CoRR*, abs/1504.02411, 2015.
- [4] Mark Braverman, Young Kun-Ko, Aviad Rubinstein, and Omri Weinstein. ETH Hardness for Densest- k -Subgraph with Perfect Completeness. In submission.
- [5] Mark Braverman, Young Kun-Ko, and Omri Weinstein. Approximating the best nash equilibrium in $n^{o(\log n)}$ -time breaks the exponential time hypothesis. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 970–982, 2015.
- [6] Yu Cheng, Ho Yee Cheung, Shaddin Dughmi, Ehsan Emamjomeh-Zadeh, Li Han, and Shang-Hua Teng. Mixture selection, mechanism design, and signaling. In *FOCS*, 2015. To appear.

- [7] Constantinos Daskalakis. On the complexity of approximating a nash equilibrium. *ACM Transactions on Algorithms*, 9(3):23, 2013.
- [8] Constantinos Daskalakis and Christos H. Papadimitriou. On oblivious ptas's for nash equilibrium. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 75–84, 2009. Full version available at <http://arxiv.org/abs/1102.2280>.
- [9] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3):12, 2007.
- [10] Shaddin Dughmi. On the hardness of signaling. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 354–363, 2014.
- [11] Russell Impagliazzo and Ramamohan Paturi. On the complexity of k-sat. *J. Comput. Syst. Sci.*, 62(2):367–375, 2001.